R E P U B L I Q U E F R A N Ç A I S E

PCT/FR 00/00465

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 21 MAR 2000
WIPO PCT

FR 00/465

09/914315

BREVET D'INVENTION

#7
03/15/03
amr

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 17 FEV. 2000

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

M Haut

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55-1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 25 FEV 1999
N° D'ENREGISTREMENT NATIONAL 9902363
DÉPARTEMENT DE DÉPÔT 75 INPI PARIS
DATE DE DÉPÔT 25 FEV. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT-SCHMIT
7 rue Le Sueur
75116 PARIS

n°du pouvoir permanent références du correspondant téléphone
014412 - OC/MN 01 40 67 11 99

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ▷ demande initiale ◁
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen
☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Dispositif d'accès sécurisé à des applications d'une carte à puce

3 DEMANDEUR (S) n° SIREN . . . . . code APE-NAF . . . .

Nom et prénoms (souligner le nom patronymique) ou dénomination

STMICROELECTRONICS S.A

Forme juridique

société anonyme

Nationalité (s) française

Adresse (s) complète (s) Pays

7, avenue Galliéni
94250 GENTILLY

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine numéro date de dépôt nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Paul BALLOT
N° 92-1009
Cabinet BALLOT-SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

BA 540 A/200298

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

014412 - OC/MN

N° D'ENREGISTREMENT NATIONAL

99 02363

TITRE DE L'INVENTION :

Dispositif d'accès sécurisé à des applications d'une carte à puce

LE(S) SOUSSIGNÉ(S)

BALLOT Paul
Cabinet BALLOT-SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

SONZOGNI Jacques

TRIMMER Mark

domiciliés au :

Cabinet BALLOT-SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Paris, le 25 février 1999

BALLOT Paul
N° 92-1009
Cabinet BALLOT-SCHMIT

BA 113/140897

OC

DISPOSITIF D'ACCES SECURISE A DES APPLICATIONS D'UNE CARTE A PUCE

La présente invention se rapporte à un dispositif d'accès sécurisé à des applications d'une carte à puce.

Plus particulièrement, l'invention concerne un dispositif d'accès sécurisé à des applications d'une carte à puce faisant intervenir notamment des instructions, informant à chaque instant sur les droits, essentiellement en terme d'accès à la mémoire de la carte à puce, de la composante logicielle ou de l'intervention matérielle qui est exécutée dans la carte à puce.

Les cartes à puce les plus courantes comprennent un microprocesseur qui gère une mémoire programme. La mémoire programme est le plus souvent dédiée à une unique application ou à un ensemble d'applications chargées en même temps dans la carte à puce. Lorsque plusieurs applications sont chargées dans une carte à puce, elles présentent une relation étroite entre elles et sont toutes destinées à un même type de service. Ainsi, par exemple, une carte à puce ne peut pas simultanément jouer le rôle de carte bancaire et le rôle de carte de fidélité pour un quelconque commerce.

Afin de ne plus être limité à un unique type d'application par carte à puce, de nouvelles architectures logicielles sont envisagées. Ces nouvelles architectures logicielles exploitent le développement de langages de programmation standardisés (par exemple, le langage "JAVA") qui résolvent les problèmes de portabilité.

La figure 1 est une représentation simplifiée d'une architecture logicielle des projets de cartes à puce qui se développent actuellement. L'architecture représentée à la figure 1 comprend notamment une

première partie 110 qui correspond à la partie dite système de l'architecture logicielle d'une carte à puce 100, et une deuxième partie 120 qui correspond à la partie dite applicative de l'architecture logicielle de la carte à puce 100. La partie système 110 de la carte à puce est essentiellement composée d'une librairie de programmes 112 du système d'exploitation de la carte à puce, d'une interface 114 pour gérer les interactions avec, par exemple, le microprocesseur de la carte à puce ou bien avec les différentes mémoires de la carte à puce, et d'un espace de gestion d'interruptions matérielles 116.

La partie applicative 120 de l'architecture logicielle est composée de différentes applications :

- une première, une deuxième, et une troisième applications principales, respectivement 122, 124 et 126;
- une première, une seconde et une troisième applications supplémentaires, respectivement 121, 123 et 125.

Les applications principales 122, 124 et 126 sont écrites dans un langage de programmation directement compréhensible par le processeur de la carte à puce.

Les applications supplémentaires 121, 123 et 125 sont typiquement des applications codées dans un langage standardisé. Ces applications peuvent être ajoutées à n'importe quel instant, à la partie système 110, dans la partie applicative 120 de l'architecture logicielle décrite. A la figure 1, les applications supplémentaires 121, 123 et 125 dépendent directement de la première application principale 122. La première application principale 122 sert ici d'interpréteur entre les applications supplémentaires et le système d'exploitation en transformant les codes des applications supplémentaires en un langage machine

compréhensible par les programmes du système d'exploitation 112.

Le dispositif d'accès sécurisé à des applications d'une carte à puce selon l'invention intervient dans une architecture de ce type.

L'architecture logicielle qui vient d'être décrite est plus complexe que celle qui existe actuellement dans les cartes à puce en circulation. En effet, l'architecture décrite suppose que l'on peut ajouter des applications dans un langage de programmation standardisé, éventuellement après la mise en circulation de la carte à puce. Un niveau satisfaisant de sécurité est par conséquent plus complexe à atteindre que lorsque une unique application, ou un groupe d'applications dédiées à une unique fonction de la carte à puce, était chargée une fois pour toutes dans la carte à puce définitivement limitée en terme d'applications disponibles. Le risque qu'une nouvelle application vienne perturber le fonctionnement des précédentes applications est en conséquence moins élevé.

La coexistence d'applications de natures diverses dans une même carte à puce peut poser un certain nombre de problèmes : par exemple, une architecture logicielle comprenant simultanément une application dédiée à l'évaluation de la fidélité d'un client à une compagnie pétrolière et une application bancaire classique, doit garantir qu'une clef secrète servant dans l'application bancaire ne peut être lue lors de l'utilisation de l'application associée à la compagnie pétrolière.

La présente invention a pour objet de pallier les problèmes qui viennent d'être décrits.

A cet effet, l'invention propose un dispositif permettant de gérer différentes applications logicielles mises en place éventuellement à différents

instants, ou différents évènements matériels, d'une carte à puce, tout en assurant une grande sécurité. Ainsi le dispositif selon l'invention offre la possibilité de détecter lorsque l'utilisateur d'une application tente d'outre-passer ses droits, par exemple en tentant d'accéder à des données qui ne sont pas destinées à l'application en question.

Pour atteindre ces objectifs, l'invention propose la mise en place d'instructions spécifiques internes au microprocesseur de la carte à puce. Ces instructions spécifiques sont des instructions d'appel (DCALL) et de retour (DRETURN). Ces instructions d'appel et de retour sont associées selon l'invention à des registres particuliers qui permettent de s'assurer du caractère autorisé ou non des opérations effectuées par l'application en cours d'exécution dans la carte à puce.

L'invention concerne donc un dispositif d'accès à des applications d'une carte à puce comprenant un microprocesseur associé à un système d'exploitation fonctionnant avec un jeu d'instructions, une mémoire de programmes et une batterie d'applications dans une mémoire de la carte à puce, caractérisé en ce qu'il comprend

- un registre du microprocesseur pour mémoriser un code, sur plusieurs bits de contrôle, propre à une entité mise en jeu,

- une instruction d'appel et une instruction de retour du jeu d'instructions pour mettre à jour instantanément et automatiquement le registre lors de l'intervention d'une nouvelle entité,

- un dispositif de contrôle pour contrôler en fonction des bits de contrôle le caractère autorisé de l'accès à des zones de la mémoire de la carte à puce

par la nouvelle entité appelée ou intervenant dans la carte à puce,

- une première liaison pour transmettre les bits de contrôle du microprocesseur vers le dispositif de contrôle.

Selon une réalisation particulière du dispositif de l'invention, chaque nouvelle entité intervenant est activée à une adresse prédéfinie d'une mémoire de type mémoire ROM (Read Only Memory dans la littérature anglaise) de la carte à puce.

Selon différents modes de réalisation de l'invention, l'entité fonctionnant dans la carte à puce peut être une application de la batterie d'applications ou un évènement matériel, ou encore le système d'exploitation associé au microprocesseur de la carte à puce.

Les différents aspects et avantages de l'invention apparaîtront plus clairement dans la suite de la description en référence aux figures qui ne sont données qu'à titre indicatif et nullement limitatif de l'invention et qui sont à présent introduites :

- la figure 1, déjà décrite, est une représentation simplifiée d'une architecture logicielle des projets de cartes à puce qui se développent actuellement,

- la figure 2 est une représentation du principe de fonctionnement selon l'invention lors de l'exécution d'une application au sein de la carte à puce.

A la figure 2, un microprocesseur 200 d'une carte à puce 100 gère l'ensemble des opérations d'une batterie d'applications 210 de la carte à puce 100.

Un bus bi-directionnel 250 assure l'échange d'informations entre le microprocesseur 200 et une quelconque application de la batterie d'applications 210. Les informations échangées peuvent être des données, des adresses ou des instructions de commande.

Un contrôleur d'accès à la mémoire 220 échange des informations avec le microprocesseur 200, notamment au moyen d'une liaison 230 qui véhicule un signal, dit signal de contrôle entre le microprocesseur 200 et le contrôleur d'accès à la mémoire 220.

Par exemple, quand une entité telle que l'application 211 requiert, au moyen du bus bi-directionnel 250, l'intervention d'une autre entité telle qu'une application 212, elle transmet une instruction d'appel DCALL suivie d'une désignation de l'entité appelée et d'un paramètre permettant de déterminer la nature de l'appel. Selon l'invention, un registre R est mis à jour lors de tels appels. Un certain nombre de bits du registre R prennent alors une valeur associée à l'entité appelée. Le registre R est donc un moyen matériel du microprocesseur 200 qui sert à mémoriser un code propre à l'entité de l'architecture logicielle qui est en train de s'exécuter, et à contrôler son domaine d'exécution.

De plus, le dispositif selon l'invention peut également prendre en compte des instructions dites matérielles, par exemple du type ré-initialisation. Les instructions dites matérielles sont des événements qui peuvent survenir en temps réel sur une carte à puce et qui génèrent des interruptions dans les microprocesseurs de ces cartes à puce. Ce type d'événement est géré par le dispositif selon l'invention de la même façon que les instructions logicielles : les bits du registre R prennent une valeur bien précise, appropriée à chaque événement en temps réel intervenant sur les cartes à puce, limitant et contrôlant ainsi les droits de ces évènements.

L'information fournie par le registre R est ainsi susceptible de contrôler une information, par exemple au microprocesseur ou à toute autre entité extérieure à

l'architecture logicielle, relative à l'identification de la zone de l'architecture logicielle concernée par l'application en cours d'exécution.

L'information fournie par le registre R permet de contrôler la zone de la mémoire de la carte à puce dans laquelle l'application à le droit d'intervenir, c'est-à-dire l'espace mémoire auquel elle peut accéder. Ainsi, un éventuel utilisateur qui tente d'utiliser de façon frauduleuse le système d'exploitation afin de récupérer des données d'une application particulière, se voit refuser l'accès à ces données. En effet, les bits du registre d'état sont, dans ce cas, différents des bits qui correspondraient à un appel DCALL de l'application particulière en question. Une confrontation entre les adresses auxquelles on tente d'accéder et les bits du registre R, communiqués par le microprocesseur au moyen de la liaison 230, est réalisée dans le contrôleur d'accès à la mémoire 220. Dans le cas où les adresses de la mémoire auxquelles on tente d'accéder ne sont pas des adresses appartenant au domaine autorisé de la dernière application ayant effectué un appel de type DCALL, une information d'accès illégal interdit l'accès à ces mémoires.

Le dispositif selon l'invention offre ainsi une grande sécurité dans le sens où des données qui sont destinées à une application ne peuvent pas être exploitées par une autre application.

Un second registre CS permet de garder en mémoire un code propre aux applications qui étaient actives au moment de la dernière instruction d'appel DCALL émise par l'application courante, c'est-à-dire celles qui sont à exécuter à la suite de l'application courante.

Lorsque l'application courante à fini de s'exécuter, une instruction de retour DRET est exécutée par le microprocesseur, et les données contenues dans

le second registre CS permettent de retourner à l'application qui s'exécutait précédemment et qui avait été activée par un appel DCALL. Le registre R est également mis à jour.

Le second registre CS ne peut être directement accédé par les applications de la carte à puce afin de garantir l'intégrité du dispositif lors de sa mise en oeuvre lors de l'exécution d'une instruction de retour DRET.

Lorsque l'application courante a fini de s'exécuter, les bits du registre R prennent une valeur spécifique à l'application qui s'exécutait précédemment, lui restituant ainsi ses droits et ses limitations en terme d'accès mémoire.

Le dispositif d'accès à des zones mémoire, selon l'invention, permet d'assurer une grande sécurité en terme d'accès aux différentes zones de la mémoire, pour une architecture logicielle telle que celle présentée à la figure 1.

REVENDICATIONS

1. Dispositif d'accès à des applications d'une carte à puce (100) comprenant un microprocesseur (200) associé à un système d'exploitation fonctionnant avec un jeu d'instructions, une mémoire de programmes et une batterie d'applications (210) dans une mémoire de la carte à puce, caractérisé en ce qu'il comprend

- un registre (R) du microprocesseur pour mémoriser un code, sur plusieurs bits de contrôle, propre à une entité mise en jeu,

- une instruction d'appel (DCALL) et une instruction de retour (DRET) du jeu d'instructions pour mettre à jour instantanément et automatiquement le registre (R) lors de l'intervention d'une nouvelle entité,

- un dispositif de contrôle (220) pour contrôler en fonction des bits de contrôle le caractère autorisé de l'accès à des zones de la mémoire de la carte à puce par la nouvelle entité appelée ou intervenant dans la carte à puce,

- une première liaison (230) pour transmettre les bits de contrôle du microprocesseur (200) vers le dispositif de contrôle (220).

2. Dispositif d'accès à des applications d'une carte à puce selon la revendication 1, caractérisé en ce qu'il comprend un second registre (CS) pour mémoriser un code propre aux applications actives au moment de la dernière instruction d'appel (DCALL) émise.

3. Dispositif d'accès à des applications d'une carte à puce selon l'une des revendications 1 ou 2, caractérisé en ce que l'entité appelée ou intervenant

dans la carte à puce est une application (211) de la batterie d'applications.

4. Dispositif selon l'une des revendications 1 ou 2, caractérisé en ce que l'entité est un évènement matériel.

FIG_1

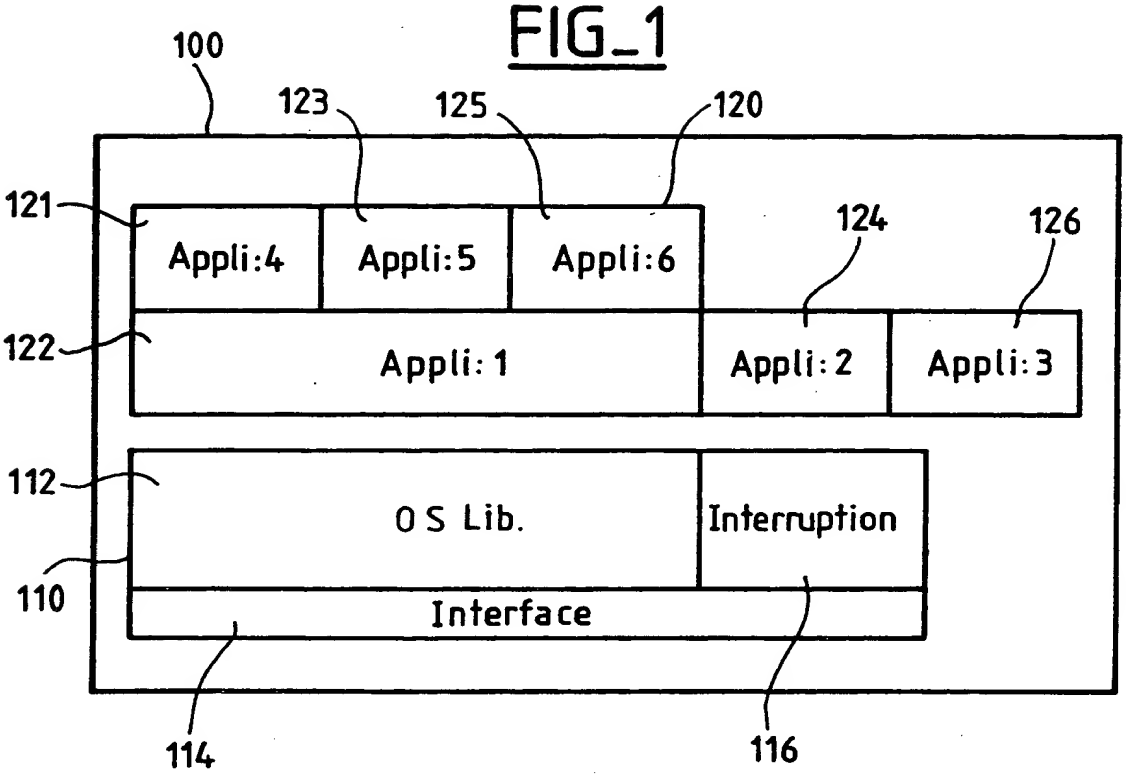
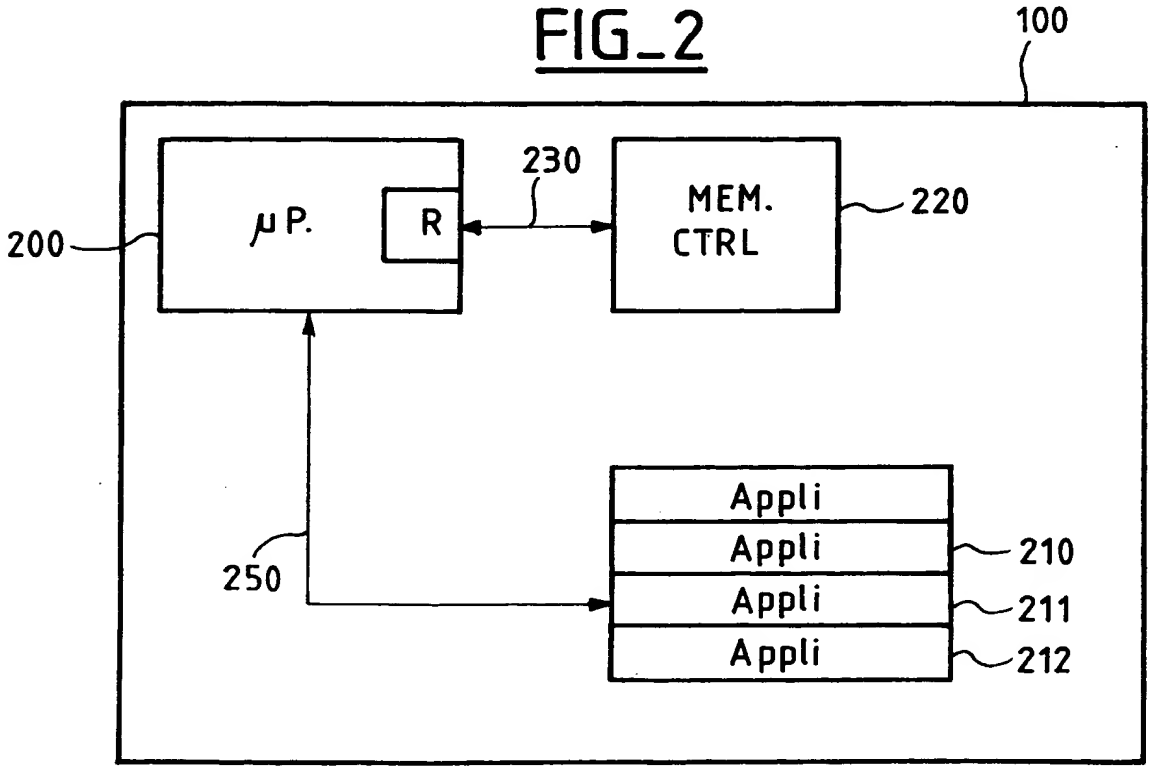

100
123
125
120
121
Appli:4
Appli:5
Appli:6
124
126
122
Appli:1
Appli:2
Appli:3
112
OS Lib.
Interruption
110
Interface
114
116

FIG_2


100
230
200
µP.
R
MEM.
CTRL
220
Appli
Appli
Appli
Appli
210
211
212
250